Identifying Incorrect Subnet Masks Using EtherPeek and EtherPeek NX

Contents

Introduction
Misconfigured subnet masks
Identifying the problem using EtherPeek
   Method 1
   Method 2
   Method 3
Conclusion

Introduction

With the proliferation of private addressing Network Address Translation (NAT) in today’s modern IP networks, subnet masks become more important than ever. Many network administrators are using the 10.x.x.x address space, but are using different subnet masks within that network. This can create problems, varying from increased utilization to machines simply being unable to access certain network resources. This document is not intended to be an in-depth guide to subnetting; rather, it is meant to demonstrate how to spot subnet mask mis-configurations using EtherPeek. (“EtherPeek” in this paper will refer to both our expert analysis EtherPeek NX and to our standard EtherPeek.) For in-depth information on all the why’s and how’s of subnetting, there are several good references on the web, such as www.howtosubnet.com and www.wildpackets.com/compendium/IP/IP-Subnt.html.

Subnet mask mis-configurations can be caused either by users statically entering the wrong IP information, or, occasionally, can be due to DHCP problems. It is easy to overlook the fact that these problems are occurring or to discount the possibility that the problems are subnet mask-related because DHCP is in use. DHCP is not a sure protection against these problems, since DHCP utilizes a database structure and this structure itself may become corrupt. Also, DHCP can be circumvented if users and junior technicians set machines to use static IP addresses and subnet masks.

Verifying correct subnet mask configuration is critical to good network health. Checking for proper subnet mask configuration should take only a few minutes a day and will enable network administrators to take appropriate action to prevent network and user slow-downs. EtherPeek is an indispensable tool for verifying subnet mask configuration. Very little knowledge of EtherPeek is needed to implement these procedures; however, if you desire, a list of formal training classes is available at www.wildpackets.com/academy.
Misconfigured subnet masks

What happens when the subnet mask is mis-configured?

When a machine is using an incorrect subnet mask one of two things will happen:

1. If a machine is configured to use a too-restrictive subnet mask, that is, more network bits or more 255’s, then a machine will not recognize that it is on the same network as machines local to it and will instead use a router rather than talk directly to the local machines. This problem is called ‘local routing’ and will at least double the bandwidth required for the conversation as well as increase the load on the router’s CPU.

   For example:

   A small network is using the network address 10.0.0.0 with a subnet mask of 255.0.0.0. This means that all addresses between 10.0.0.1 and 10.255.255.254 are directly reachable by any device in the network.

   A machine that was using an address of 10.0.0.1 and a mask of 255.255.255.0 would only be able to reach addresses 10.0.0.1 through 10.0.0.254. To contact any other machine on the network the packet would be sent to the router.

2. The corollary to this problem is a machine whose subnet mask is not restrictive enough. This problem will result in a machine believing that certain addresses are actually on its local network when they are not. That is, a packet should be sent to the router for delivery to those addresses. The result is a machine not being able to reach certain resources.

   For example:

   A small network is using the network address 10.0.0.0 with a subnet mask of 255.255.255.0. This means that all addresses between 10.0.0.1 and 10.0.0.254 are directly reachable by any device in the network. A machine using an address of 10.0.0.1 and a mask of 255.0.0.0 would think itself able to reach any addresses 10.0.0.1 through 10.255.255.254 directly, when in actuality the packet might have to be sent to the router for delivery to a different subnet.

A third problem might arise as well. When a machine sees an IP broadcast it examines the IP address and checks to make sure that it is actually the broadcast address for that segment. In the previous examples, there would be two different local subnet broadcast addresses based on the different masks: 10.255.255.255 and 10.0.0.255. Machines configured to use one address would not see the other as a broadcast. Instead, they could view it as a node address and either ignore it, or worse, try to ARP for that address in an attempt to forward it (this typically occurs when machines are running routing processes). In the Windows world, this problem often prevents machines from being able to browse the network neighborhood.

Identifying the problem using EtherPeek

Using the detail statistics of EtherPeek makes subnet mask errors easy to spot, and there are several methods you may use. You can even use these techniques to create automated alarms to instantly notify you of the mis-configured machines.
Method 1

The first method uses the detail window of the nodes display from either a capture file or the Statistics menu. From the nodes display, find the Ethernet address FF:FF:FF:FF:FF:FF. It might also be labeled Ethernet Broadcast. If there is a plus sign next to it, click to expand the list of associated IP addresses.

The result is a display of all IP broadcast addresses associated with the Ethernet broadcast address. The bottom portion of each line shows the percentage of broadcasts to that address. These are the broadcast IP addresses in this network. If you have more than 255.255.255.255 and the correct one for your environment (e.g. 10.255.255.255) then you have identified a problem.

Double-clicking on these extra IP broadcast addresses will open a dialog box showing which nodes are sending to the associated IP broadcast address. You can then track down and reconfigure those machines.
Method 2

Another easy method for tracking down machines with this problem is via the use of a protocol called ICMP. A router will typically use ICMP to inform a device that it is not necessary to send a packet to it, and to direct that device to instead send it either directly or via another router. This is called an ICMP Redirect and is only one of the many messages that ICMP can send. Finding these ICMP messages is easy to do using the protocol tab. From the protocol tab, search the directory tree of protocols for Redirect (Ethernet Type 2, IP, ICMP, Redirect). Right-click on Redirect and from the resulting menu choose Select Related Packets > By Protocol.
This will return you to the packets window and give you the option of hiding either the selected or unselected packets. Choose Hide Unselected. The resulting list of packets was sent from your routers to your workstations to inform them of a better route.

Examining the individual packets shows you where the user was trying to go and how they should get there next time. Sadly, many operating systems ignore these packets and continue the same behavior. Luckily, many routers will only send a limited number of these redirect packets, realizing that these nodes are a lost cause.
Method 3

A third method for quickly and proactively monitoring for stations using the wrong IP broadcast address is to set up a filter to search them out. You can accomplish this by creating an advanced filter looking for IP packets being sent to the Ethernet broadcast address but not to the correct IP broadcast address. So if your broadcast address were 10.1.1.255, the filter would look like this:
Note: Make certain that all of the above address filters look like this one with regard to the "Address 2 to 1" button, and the "Any address" button, below.

After creating this filter, your next steps are to:

1. Open a new capture window.
2. Select the Filters tab.
3. Click on the newly created filter.
4. Click the Start Capture button.

5. Return to the Packets tab.

Any packets in this new window are from machines with incorrectly configured subnet masks. By selecting the nodes tab (then clicking on the Node column header to sort) you can easily obtain a list of all of the associated IP and Ethernet addresses. In the above example, the mask was set to 255.255.255.240.
Conclusion

By verifying and correcting these subnet mask problems, your network can see vastly improved performance. The techniques discussed above are just a few of the ways you can use EtherPeek for uncovering these problems, and require very little experience with the tool. Even more powerful solutions exist for expert users of EtherPeek, and several training classes are available from WildPackets Academy to help you explore the full range of solutions this software offers to power-users. EtherPeek can also assist you in identifying many other problems that may arise in your network. These problems include, but are not limited to: intrusion detection, slow client or server performance, and proactive performance monitoring. After training and experience, users can even automate the reporting of these errors through email or page notification sent out to alert the helpdesk.
WildPackets Professional Services

WildPackets offers a full spectrum of unique professional support services, available on-site, online or through remote dial-in service.

WildPackets Academy

WildPackets Academy provides the most effective and comprehensive network and protocol analysis training available, meeting the professional development and training requirements of corporate, educational, government, and private network managers. Our instructional methodology and course design centers around practical applications of protocol analysis techniques for Ethernet and 802.11 wireless LANs.

In addition to classroom-taught Network Analysis Courses, WildPackets Academy also offers:

• Web-Delivered Training
• On-site and Custom Courseware Delivery
• The Technology, Engineering, and Networking Video Workshop Series
• On-site and Remote Consulting Services
• Instruction and testing for the Network Analysis Expert (NAX™) Certification

For more information about consulting and educational services, including complete course catalog, pricing and scheduling, please visit www.wildpackets.com/academy. NAX examination and certification details are available at www.nax2000.com.

Live Online Quick Start Program

WildPackets now offers one-hour online Quick Start Programs on using EtherPeek NX/EtherPeek and AiroPeek NX/AiroPeek, led by a WildPackets Academy Instructor. Please visit www.wildpackets.com for complete details and scheduling information.

About WildPackets, Inc.

WildPackets, a privately-held corporation, was founded in 1990 with a mission to create software-based tools to simplify the complex tasks associated with maintaining, troubleshooting, and optimizing evolving computer networks. WildPackets' patented, core "Peek" technology is the development base for EtherPeek™, TokenPeek™, AiroPeek™, and the NX™ family of expert packet analyzers. All are recognized as the analysis tools of choice for small, medium, and large enterprise customers, allowing IT Professionals to easily maximize network productivity. Information on WildPackets, WildPackets Academy, Professional Services, products, and partners is available at www.wildpackets.com.